МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
Педагогическим советом колледжа

протокол № 4 от 18.11.2025 г.

Директор колледжа _____ А.Э.Чечулин
(подпись)

Утверждена
Советом по учебно-методическим вопросам и качеству образования

протокол № 4 от 16.12.2025 г.

Председатель _____ Д.А. Карх
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	ОП.05 Основы информационной безопасности
Специальность	09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ
Форма обучения	очная
Год набора	2026

Разработана:
Преподаватель
Н.С. Наштатик

Екатеринбург
2026 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной образовательной программысреднего профессионального образования - программы подготовки специалистов среднего звена,разработанной в соответствии с ФГОС СПО

ФГОС СПО	Федеральный государственный образовательный стандарт среднегопрофессионального образования по специальности 09.02.11 РАЗРАБОТКА ИУПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ (приказ МинобрнаукиРоссии от 24.02.2025 г. № 138)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины «Основы информационной безопасности»: формирование у обучающихсязнаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствахзащищаемой информации, основных информационных угрозах, существующих направленияхзащиты и возможностях построения моделей, стратегий, методов и правил информационнойзащиты.

В результате освоения дисциплины обучающийся должен иметь:

Умения:

- анализировать предметную область и выделять основные сущности;
- определять требования к базе данных;
- разрабатывать концептуальную, логическую и физическую модели баз данных;
- проектировать схему базы данных;
- работать с современными case-средствами проектирования баз данных;
- определять связи между таблицами;
- определять типы данных для полей таблиц;
- оформление документации на спроектированную базу данных
- создавать и удалять базы данных;
- создавать пользователей и назначать права доступа;
- обеспечивать безопасность баз данных;
- обеспечивать безопасность и управлять доступом к данным;
- создавать и восстанавливать резервные копии данных;
- разрабатывать и внедрять системы защиты баз данных от несанкционированногодоступа;
- разрабатывать и внедрять системы резервного копирования и восстановления базданных;
- проводить аудит безопасности баз данных;
- устанавливать и настраивать механизмы аутентификации и авторизации пользователей;
- создавать и управлять ролями и правами доступа к данным;
- шифровать данные и обеспечивать их конфиденциальность;
- контролировать целостность данных и обнаруживать изменения;
- использовать механизмы аудита для отслеживания доступа к данным;
- использовать механизмы мониторинга для обнаружения угроз безопасности;
- создавать и управлять защищенными соединениями с базой данных;
- использовать механизмы защиты от SQL-инъекций и других видов атак;
- создавать и управлять бэкапами и резервными копиями данных;
- обеспечивать безопасность базы данных при использовании облачных сервисов
- проводить сбор и анализ исходных данных для разработки проектной документации наинформационную систему;
- определять требования и функциональность информационной системы на основесобранных данных;
- анализировать требований безопасности информационных систем;
- разрабатывать и реализовывать подсистемы безопасности информационных систем;
- тестировать и проводить отладку подсистем безопасности информационных

- разрабатывать скрипты и/или программные модули для тестирования по, в том числедля проверки информационной безопасности разрабатываемого ПО;

Знания:

- основные положения теории баз данных, хранилищ данных, баз знаний;
- основные принципы структуризации и нормализации базы данных;
- основные принципы построения концептуальной, логической и физической моделиданных;
- методы описания схем баз данных в современных системах управления базамиданных;
- структуру данных систем управления базами данных, основные понятия и принципыпроектирования баз данных;
- структуру реляционной базы данных;
- архитектуру СУБД;
- основные принципы администрирования баз данных;
- принципы резервного копирования и восстановления баз данных;
- методы защиты баз данных от внешних угроз;
- особенности работы с различными СУБД;
- Язык SQL (Structured Query Language);
- управление транзакциями и контроль целостности данных;
- управление доступом и безопасностью баз данных;
- резервное копирование и восстановление данных
- методы защиты баз данных от несанкционированного доступа;
- методы создания и восстановления резервных копий баз данных;
- особенности работы с различными типами СУБД;
- методы проведения аудита безопасности баз данных;
- принципы криптографии и методов шифрования данных;
- стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;
- методы аутентификации и авторизации пользователей, включая использованиепаролей, сертификатов и биометрических данных;
- методы контроля доступа, включая создание ролей и групп пользователей, управлениеправами доступа и аудит доступа к данным;
- методы обнаружения и предотвращения атак, включая защиту от SQL-инъекций,DoS/DDoS-атак и других угроз безопасности;
- методы мониторинга и анализа журналов событий для обнаружения угрозбезопасности и анализа производительности базы данных;
- методы создания и управления защищенными соединениями с базой данных, включаяVPN-туннели и SSL-шифрование;
- методы создания и управления бэкапами и резервными копиями данных, включаяиспользование инкрементальных и дифференциальных бэкапов;
- методы обеспечения безопасности базы данных при использовании облачныхсервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам;
- законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.
- анализировать требований безопасности информационных систем;
- разрабатывать и реализовывать подсистемы безопасности информационных систем;
- тестировать и проводить отладку подсистем безопасности информационных систем
- принципы безопасности информационных систем;
- современные методы и технологии в области безопасности информационных систем;
- законодательных и нормативных актов в области безопасности информационныхсистем
- российские и международные стандарты тестирования информационных систем;
- требования по обеспечению безопасности аппаратных и программных средствавтоматизированных систем, используемых при выполнении тестовых процедур, включая вопросыантивирусной защиты;

ГВ 4: Ориентированный на активное гражданское участие в социально-политическихпроцессах на основе уважения закона и правопорядка, прав и свобод сограждан.

ПВ 3: Проявляющий деятельное ценностное отношение к историческому и культурномунаследию своего и других народов России, их традициям, праздникам.

ПВ 4: Проявляющий уважение к соотечественникам, проживающим за рубежом,поддерживающий их права, защиту их интересов в сохранении общероссийской идентичности.

ФВ 2: Соблюдающий правила личной и общественной безопасности, в том числе безопасногоповедения в информационной среде.

ФВ 3: Выражающий на практике установку на здоровый образ жизни (здоровое питание,соблюдение гигиены, режим занятий и отдыха, регулярную физическую активность), стремление кфизическому совершенствованию.

ФВ 4: Проявляющий сознательное и обоснованное неприятие вредных привычек (курения,употребления алкоголя, наркотиков, любых форм зависимостей), деструктивного поведения вобществе и цифровой среде, понимание их вреда для физического и психического здоровья.

ПТВ 2: Участвующий в социально значимой трудовой и профессиональной деятельностиразного вида в семье, образовательной организации, на базах производственной практики, в своейместности.

ПТВ 3: Выражающий осознанную готовность к непрерывному образованию исамообразованию в выбранной сфере профессиональной деятельности.

ПТВ 4: Понимающий специфику профессионально-трудовой деятельности, регулированиятрудовых отношений, готовый учиться и трудиться в современном высокотехнологичном мире наблаго государства и общества.

ПТВ 7В: Экономически активный, предприимчивый, готовый к самозанятости.

ЦНП 1: Деятельно выражающий познавательные интересы в разных предметных областях сучётом своих интересов, способностей, достижений, выбранного направления профессиональногообразования и подготовки.

ЦНП 2: Обладающий представлением о современной научной картине мира, достиженияхнауки и техники, аргументированно выражающий понимание значения науки и технологий дляразвития российского общества и обеспечения его безопасности.

ЦНП 3: Демонстрирующий навыки критического мышления, определения достоверностинаучной информации, в том числе в сфере профессиональной деятельности.

ЦНП 4: Умеющий выбирать способы решения задач профессиональной деятельностиприменительно к различным контекстам.

ЦНП 5: Использующий современные средства поиска, анализа и интерпретации информации,информационные технологии для выполнения задач профессиональной деятельности.

ЦНП 6: Развивающий и применяющий навыки наблюдения, накопления и систематизациифактов, осмысления опыта в естественнонаучной и гуманитарной областях познания,исследовательской и профессиональной деятельности.

ЦНП 7В: Признающий ценность непрерывного образования, ориентирующийся визменяющемся рынке труда, избегающий безработицы; управляющий собственнымпрофессиональным развитием; рефлексивно оценивающий собственный жизненный опыт,

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточнаяаттестация	Часов					
	Всего засеместр	Контактная работа .(поуч.зан.)			Самостоятельная работа в том числеподготовкаконтрольных икурсовых	
		Всего	Лекции	Лабораторные		
Семестр 4						
Зачет с оценкой	96	92	46	46	4	0

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ООП

В результате освоения ООП у выпускника должны быть сформированы компетенции,установленные в соответствии ФГОС СПО.

Общие компетенции (ОК)

Шифр и наименованиекомпетенции	Индикаторы достижения компетенций
ОК 01. Выбирать способырешения задачпрофессиональнойдеятельностиприменительно к различнымконтекстам	Умения: - распознавать задачу и/или проблему в профессиональном и/илисоциальном контексте - анализировать задачу и/или проблему и выделять её составныечасти - определять этапы решения задачи - выявлять и эффективно искать информацию, необходимую длярешения задачи и/или проблемы - составлять план действия - определять необходимые ресурсы - владеть актуальными методами работы в профессиональной исмежных сферах - реализовывать составленный план Знания: - актуальный профессиональный и социальный контекст, вкотором приходится работать и жить - основные источники информации и ресурсы для решения задачи проблем в профессиональном и/или социальном контексте - алгоритмы выполнения работ в профессиональной и смежныхобластях - методы работы в профессиональной и смежных сферах
ОК 02. Использоватьсовременные средствапоиска, анализа иинтерпретацииинформации, иинформационныетехнологии для выполнениязадач профессиональнойдеятельности	Умения: - определять задачи для поиска информации - определять необходимые источники информации - планировать процесс поиска - структурировать получаемую информацию - выделять наиболее значимое в перечне информации - оценивать практическую значимость результатов поиска Знания: - номенклатура информационных источников, применяемых впрофессиональной деятельности

ОК 09. Пользоватьсяпрофессиональнойдокументацией нагосударственном иностранном языках	Умения: - понимать общий смысл четко произнесенных высказываний наизвестные темы (профессиональные и бытовые), понимать тексты набазовые профессиональные темы - участвовать в диалогах на знакомые общие и профессиональныетемы - строить простые высказывания о себе и о своейпрофессиональной деятельности - кратко обосновывать и объяснять свои действия (текущие ипланируемые) - писать простые связные сообщения на знакомые илиинтересующие профессиональные темы Знания: - правила построения простых и сложных предложений напрофессиональные темы - основные общеупотребительные глаголы (бытовая ипрофессиональная лексика) - лексический минимум, относящийся к описанию предметов,средств и процессов профессиональной деятельности

Профессиональные компетенции (ПК)

Шифр и наименованиекомпетенции	Индикаторы достижения компетенций
проектирование и разработка информационных систем (по выбору)	
ПК 3.1. Собирать исходныеданные для разработкипроектной документации наинформационную систему	Умения: - проводить сбор и анализ исходных данных для разработкипроектной документации на информационную систему; - определять требования и функциональность информационнойсистемы на основе собранных данных; Знания: - современные стандарты информационного взаимодействиясистем; - программные средства и платформы
ПК 3.3. Разрабатыватьподсистемы безопасностиинформационной системы всоответствии с техническимзаданием	Умения: - анализировать требований безопасности информационныхсистем; - разрабатывать и реализовывать подсистемы безопасностиинформационных систем; - тестировать и проводить отладку подсистем безопасностиинформационных систем Знания: - принципы безопасности информационных систем; - современные методы и технологии в области безопасностиинформационных систем; - законодательных и нормативных актов в области безопасностиинформационных систем

ПК 3.6. Осуществлятьмодульное иинтеграционноетестированиеинформационной системы	Умения: - разрабатывать скрипты и/или программные модули длятестирования по, в том числе для проверки информационнойбезопасности разрабатываемого ПО; Знания: - российские и международные стандарты тестированияинформационных систем; - требования по обеспечению безопасности аппаратных ипрограммных средств автоматизированных систем, используемых привыполнении тестовых процедур, включая вопросы антивирусной защиты; - тестовые данные, обеспечивающие проверку
разработка, администрирование и защита баз данных	
ПК 1.1. Проектировать базыданных	Умения: - анализировать предметную область и выделять основныесущности; - определять требования к базе данных; - разрабатывать концептуальную, логическую и физическуюмодели баз данных; - проектировать схему базы данных; - работать с современными case-средствами проектирования базданных; - определять связи между таблицами; - определять типы данных для полей таблиц; - оформление документации на спроектированную базу данных Знания: - основные положения теории баз данных, хранилищ данных, баззнаний; - основные принципы структуризации и нормализации базыданных; - основные принципы построения концептуальной, логической ифизической модели данных; - методы описания схем баз данных в современных системахуправления базами данных; - структуру данных систем управления базами данных, основныепонятия и принципы

ПК 1.4. Администрироватьбазы данных	Умения: - создавать и удалять базы данных; - создавать пользователей и назначать права доступа; - обеспечивать безопасность баз данных; - обеспечивать безопасность и управлять доступом к данным; - создавать и восстанавливать резервные копии данных; Знания: - архитектуру СУБД; - основные принципы администрирования баз данных; - принципы резервного копирования и восстановления базданных; - методы защиты баз данных от внешних угроз; - особенности работы с различными СУБД; - Язык SQL (Structured Query Language); - управление транзакциями и контроль целостности данных; - управление доступом и безопасностью баз данных; - резервное копирование и восстановление данных;

ПК 1.5. Защищатьинформацию в базе данныхс использованиемтехнологии защитыинформации	Умения: - разрабатывать и внедрять системы защиты баз данных отнесанкционированного доступа; - разрабатывать и внедрять системы резервного копирования ивосстановления баз данных; - проводить аудит безопасности баз данных; - устанавливать и настраивать механизмы аутентификации иавторизации пользователей; - создавать и управлять ролями и правами доступа к данным; - шифровать данные и обеспечивать их конфиденциальность; - контролировать целостность данных и обнаруживать изменения; - использовать механизмы аудита для отслеживания доступа кданным; - использовать механизмы мониторинга для обнаружения угрозбезопасности; - создавать и управлять защищенными соединениями с базойданных; - использовать механизмы защиты от SQL-инъекций и другихвидов атак; - создавать и управлять бэкапами и резервными копиями данных; - обеспечивать безопасность базы данных при использованииоблачных сервисов Знания: - методы защиты баз данных от несанкционированного доступа; - методы создания и восстановления резервных копий базданных; - особенности работы с различными типами СУБД; - методы проведения аудита безопасности баз данных; - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH,Kerberos и др.; - методы аутентификации и авторизации пользователей, включаяиспользование паролей, сертификатов и биометрических данных; - методы контроля доступа, включая создание ролей и групппользователей, управление правами доступа и аудит доступа к данным; - методы обнаружения и предотвращения атак, включая защиту отSQL-инъекций, DoS/DDoS-атак и других угроз безопасности; - методы мониторинга и анализа журналов событий дляобнаружения угроз безопасности и анализа производительности базыданных; - методы создания и управления защищенными соединениями сбазой данных, включая VPN-туннели и SSL-шифрование; - методы создания и управления бэкапами и резервными копиямиданных, включая использование инкрементальных идифференциальных бэкапов; - методы обеспечения безопасности базы данных прииспользовании облачных сервисов, включая защиту от утечки данныхи управление доступом к облачным ресурсам; - законодательство и стандарты безопасности, такие как GDPR,HIPAA, PCI DSS и др.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост.работа	Контрольсамостоятельной работы
			Лекции	Лабораторные	Практическиезанятия		
Семестр 4		96					
Тема 1.	Введение в информационнуюбезопасность (ГВ 4, ПВ 3, ПВ 4, ФВ2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4,ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ	2	2				
Тема 2.	Управление безопасностью информации(ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4,ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	6	6				
Тема 3.	Криптография (ГВ 4, ПВ 3, ПВ 4, ФВ2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4,ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	18	8	8		2	
Тема 4.	Защита сетевой инфраструктуры (ГВ 4,ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2,ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2,ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	14	6	8			
Тема 5.	Безопасность приложений (ГВ 4, ПВ 3,ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3,ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	10	4	6			
Тема 6.	Защита данных (ГВ 4, ПВ 3, ПВ 4, ФВ2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4,ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	14	6	8			
Тема 7.	Безопасность облачных технологий (ГВ4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2,ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2,ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1,	10	4	6			

Тема 8.	Инциденты безопасности (ГВ 4, ПВ 3,ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3,ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5,	12	4	6		2	
Тема 9.	Социальная инженерия и человеческийфактор (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3,ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В,ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК3.1, ПК 3.3, ПК 3.6)	6	2	4			
Тема10.	Будущее информационной безопасности(ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4,ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1,ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК3.1, ПК 3.3, ПК 3.6)	4	4				

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочногосредст	Описание оценочного средства	Критериоценивания
Текущий контроль (Приложение 4)			
Тема 1 - 3	Тест	Тест состоит из 10 вопросов закрытого типа.Количество вариантов - 2.	Оценивается от 2до 5 баллов
Тема 1 - 3	Практическаяработа	Работа состоит из 2 вариантов по 1 заданию вкаждом варианте.	Оценивается от 2до 5 баллов
Тема 4	Вопросы	Письменный опрос по вопросам. Количествовопросов - 5. Количество вариантов - 2.	Оценивается от 2до 5 баллов
Тема 4	Практическаяработа	Работа состоит из 1 задания.	Оценивается от 2до 5 баллов
Тема 5	Тест	Тест состоит из 10 вопросов закрытого типа.Количество вариантов - 2.	Оценивается от 2до 5 баллов
Тема 5	Практическаяработа	Работа состоит из 1 задания.	Оценивается от 2до 5 баллов
Тема 6–7	Вопросы	Письменный опрос по вопросам. Количествовопросов - 5. Количество вариантов - 2.	Оценивается от 2до 5 баллов
Тема 6–7	Практическаяработа	Работа состоит из 1 задания.	Оценивается от 2до 5 баллов
Тема 8–10	Тест	Тест состоит из 10 вопросов закрытого типа.Количество вариантов - 2.	Оценивается от 2до 5 баллов
Тема 8–10	Практическаяработа	Работа состоит из 2 вариантов по 1 заданию вкаждом варианте.	Оценивается от 2до 5 баллов

Промежуточная аттестация (Приложение 5)			
4 семестр(ЗаО)	Билет для дифференцированного зачета	Билет состоит из трех вопросов: 1теоретический вопрос, 3 тестовых задания, 1практическое задание. Количество билетов -25.	Оценивается от 2до 5 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ООП формируется на основе объединения текущего контроля ипромежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показываетуровень подготовки студента.

Текущий контроль. Используется 5-балльная система оценивания. Оценка работы студента втечении семестра осуществляется преподавателем в соответствии с разработанной им системойоценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин (предметов) и практик закреплены виды текущегоконтроля, планируемые результаты контрольных мероприятий и критерии оценки учебныйдостижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, пооценке деятельности студента.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работыстудента по окончанию дисциплины (части дисциплины) осуществляется преподавателем всоответствии с разработанной им системой оценки достижений студента в процессе обучения поданной дисциплине. Промежуточная аттестация также проводится по окончанию формированиякомпетенций.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Могут быть допущены недочеты, исправленныестудентом самостоятельно в процессе работы (ответаи т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеютприменять, исследовать, идентифицировать,анализировать, систематизировать, распределять покатегориям, рассчитать показатели,классифицировать, разрабатывать модели,алгоритмизировать, управлять, организовать,планировать процессы исследования, осуществлятьоценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняетсяисправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическимизнаниями, не умеют самостоятельно применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Не сформированы умения и навыки для
100% - 50%	зачтено	характеристика показателя соответствует «отлично»,«хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует«неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Введение в информационную безопасность (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2,ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Основные понятия и определения. История и развитие информационной безопасности.Актуальные угрозы и риски в информационной безопасности»
Тема 2. Управление безопасностью информации (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3,ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Нормативно-правовое регулирование в области информационной безопасности. Основныетребования законодательства и правовые основы защиты информации» Лекция «Политики и процедуры безопасности. Организация внутреннего регулирования процессовинформационной безопасности» Лекция «Оценка рисков и управление ими. Методы выявления, анализа и минимизации рисковинформационной безопасности»
Тема 3. Криптография (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Основы криптографии. Симметричные и асимметричные алгоритмы и принципы ихприменения» Лекция «Хэширование и цифровые подписи. Обеспечение целостности, подлинности инеотказуемости информации» Лекция «Применение криптографии в приложениях. Использование криптографических механизмовв современных информационных системах» Лекция «Стеганография. Методы скрытой передачи информации и особенности их применения»
Тема 4. Защита сетевой инфраструктуры (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4,ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Основы сетевой безопасности. Базовые принципы защиты сетевой инфраструктуры исетевого взаимодействия» Лекция «Защита от атак на сетевую инфраструктуру. Противодействие DDoS, MITM и другим типамсетевых атак» Лекция «Использование VPN и межсетевых экранов. Средства организации защищённого сетевогодоступа и фильтрации трафика»
Тема 5. Безопасность приложений (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Уязвимости веб-приложений. Анализ OWASP Top Ten и типовых угроз безопасностиприложений» Лекция «Безопасное программирование. Лучшие практики разработки защищённых программныхрешений»

Тема 6. Защита данных (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Шифрование данных в покое и в транзите. Методы защиты информации при хранении ипередаче» Лекция «Резервное копирование и восстановление данных. Обеспечение сохранности информации ивосстановление после сбоев» Лекция «Управление доступом к данным. Принципы разграничения прав и контроля доступа кинформационным ресурсам»
Тема 7. Безопасность облачных технологий (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3,ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Особенности безопасности в облачных средах. Основные риски и механизмы защитыинформации в облачной инфраструктуре» Лекция «Модели облачных услуг и их безопасность. Особенности обеспечения безопасности в IaaS,PaaS и SaaS»
Тема 8. Инциденты безопасности (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Реакция на инциденты и управление ими. Анализ инцидентов, цифровая криминалистика,OSINT и форензика» Лекция «Восстановление после инцидента. Кибербезопасность, расследование последствий атак ипротиводействие промышленному шпионажу»
Тема 9. Социальная инженерия и человеческий фактор (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2,ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Психология атак: социальная инженерия. Обучение сотрудников вопросаминформационной безопасности и снижение влияния человеческого фактора»
Тема 10. Будущее информационной безопасности (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3 , ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6) Лекция «Тенденции и новые технологии в области безопасности. Применение AI, ML и блокчейна вразвитии современных систем защиты информации» Лекция «Этические аспекты информационной безопасности. Перспективы развития средств иметодов защиты информации в условиях цифровой трансформации»

7.2 Содержание практических занятий и лабораторных работ

Тема 3. Криптография (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №1 «Работа с симметричными алгоритмами шифрования. Изучение принциповшифрования данных с использованием одного секретного ключа. Анализ особенностей применениясимметричных алгоритмов в задачах защиты информации»

Лабораторная работа №2 «Работа с асимметричными алгоритмами шифрования. Освоениепринципов использования открытого и закрытого ключей для защиты данных. Сравнениевозможностей асимметричных криптосистем при решении практических задач»

Лабораторная работа №3 «Хэширование данных. Вычисление хэш-значений для различныхсообщений и анализ изменения результата при модификации исходных данных. Исследование ролихэширования в обеспечении целостности информации»

Лабораторная работа №4 «Создание цифровой подписи сообщения. Формирование и проверкаэлектронной подписи для подтверждения подлинности документа. Изучение механизмовобеспечения целостности и неотказуемости информации»

Тема 4. Защита сетевой инфраструктуры (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4,ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №5 «Организация защиты от сетевых атак. Выявление базовых угроз сетевойинфраструктуре и определение мер противодействия. Анализ способов снижения рисканесанкционированного доступа»

Лабораторная работа №6 «Противодействие DDoS и MITM-атакам. Изучение признаков сетевыхатак и базовых методов защиты от них. Оценка эффективности различных механизмов фильтрации ипредотвращения перехвата данных»

Лабораторная работа №7 «Организация работы VPN. Настройка защищённого канала связи длябезопасной передачи данных. Анализ назначения VPN в корпоративной и удалённой работе»

Лабораторная работа №8 «Организация работы межсетевого экрана. Настройка правил фильтрациисетевого трафика и разграничения доступа. Оценка роли межсетевого экрана в защите локальнойсети»

Тема 5. Безопасность приложений (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №9 «Анализ уязвимостей веб-приложений по модели OWASP Top Ten.Выявление наиболее распространённых категорий угроз в прикладных системах. Подготовкавыводов о критичности обнаруженных проблем»

Лабораторная работа №10 «Анализ уязвимостей программного приложения. Проверка приложенияна наличие типовых ошибок реализации и конфигурации. Подготовка отчёта с описаниемнайденных недостатков безопасности»

Лабораторная работа №11 «Тестирование на проникновение приложений. Исследование доступныхточек входа и выявление потенциальных уязвимостей. Формирование рекомендаций по повышениюуровня защищённости приложения»

Тема 6. Защита данных (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1,ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №12 «Шифрование данных в покое и в транзите. Исследование методовзащиты информации при хранении и передаче. Сравнение подходов к обеспечениюконфиденциальности данных в различных условиях»

Лабораторная работа №13 «Выполнение резервного копирования данных. Настройка процедурысоздания резервных копий для обеспечения сохранности информации. Оценка требований кпериодичности и надёжности резервирования»

Лабораторная работа №14 «Восстановление данных после сбоя. Отработка процедуры возвратаинформации из резервной копии. Проверка полноты и корректности восстановленных данных»

Лабораторная работа №15 «Управление доступом к данным. Настройка прав пользователей иразграничение доступа к информационным ресурсам. Анализ принципа минимальных привилегийпри работе с данными»

Тема 7. Безопасность облачных технологий (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3,ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №16 «Анализ безопасности облачной среды. Выявление основных угроз прихранении и обработке данных в облаке. Подготовка предложений по усилению защиты облачныхресурсов»

Лабораторная работа №17 «Настройка базовых параметров безопасности облачного сервиса.Управление доступом к облачным ресурсам и контроль действий пользователей. Оценка влияниявыбранных настроек на общий уровень защищённости»

Лабораторная работа №18 «Изучение моделей облачных услуг IaaS, PaaS и SaaS. Сравнениеособенностей разных моделей с точки зрения защиты информации. Анализ механизмовбезопасности, применяемых в облачной среде»

Тема 8. Инциденты безопасности (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №19 «Работа с инцидентами информационной безопасности. Классификацияинцидентов и определение порядка реагирования на них. Отработка последовательности действийпри выявлении нарушения безопасности»

Лабораторная работа №20 «Анализ инцидента методами цифровой криминалистики. Сбор ипервичное исследование цифровых следов инцидента. Подготовка заключения по фактам нарушениябезопасности»

Лабораторная работа №21 «Восстановление после инцидента безопасности. Разработка мер полокализации последствий и восстановлению работоспособности системы. Анализ значимостирезервных механизмов и планов восстановления»

Тема 9. Социальная инженерия и человеческий фактор (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2,ПТВ 3, ПТВ 4, ПТВ 7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)

Лабораторная работа №22 «Анализ сценариев атак социальной инженерии. Выявлениепсихологических механизмов воздействия на пользователя и признаков манипуляции. Оценкауязвимости персонала к таким атакам»

Лабораторная работа №23 «Разработка политики информационной безопасности для сотрудников.Формирование правил безопасной работы с информацией и цифровыми ресурсами. Определениетребований к поведению пользователей в организации»

7.3. Содержание самостоятельной работы

Тема 8. Инциденты безопасности (ГВ 4, ПВ 3, ПВ 4, ФВ 2,ФВ 3, ФВ 4, ПТВ 2, ПТВ 3, ПТВ 4, ПТВ7В, ЦНП 1, ЦНП 2, ЦНП 3
, ЦНП 4, ЦНП 5, ЦНП 6, ЦНВ 7В, ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.3, ПК 3.6)
Самостоятельная работа «Анализ инцидентов информационной безопасности и методовреагирования на них. Изучение этапов обработки инцидента, принципов цифровой криминалистикии подходов к восстановлению после нарушения безопасности. Подготовка предложений посовершенствованию мер реагирования и предупреждения инцидентов»

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки кзачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ

http://lib.usue.ru/

Основная литература:

2. Часовских В. П., Акчурина Г. А., Лабунец В. Г., Стариков Е. Н., Кох Е. В.Администрирование и кибербезопасность информационных систем [Электронный ресурс]:учебноепособие. - Екатеринбург: УрГЭУ, 2022. - 172, [1] – Режим доступа:http://lib.wbstatic.usue.ru/resource/limit/ump/24/p496302.pdf

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации[Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2025. - 336 – Режимдоступа: https://znanium.com/catalog/product/2178344

4. Шустова Л.И., Тараканов О.В. Базы данных [Электронный ресурс]:Учебник. - Москва:ООО "Научно-издательский центр ИНФРА-М", 2026. - 304 – Режим доступа:https://znanium.com/catalog/product/2216840

5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронныйресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2026. - 416 –Режим доступа: https://znanium.com/catalog/product/2207574

Дополнительная литература:

2. Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю.Криптографическая защита информации [Электронный ресурс]:Учебное пособие : Учебноепособие. - Москва: Издательский Центр РИО, 2025. - 321 – Режим доступа:https://znanium.com/catalog/product/2169480

3. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронныйресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 349 – Режим доступа:https://urait.ru/bcode/561077

4. Кудрина Е. В., Огнева М. В. Основы алгоритмизации и программирования на языке C#[Электронный ресурс]:учебник для спо. - Москва: Юрайт, 2025. - 322 – Режим доступа:https://urait.ru/bcode/565504

5. Хорев П. Б. Программно-аппаратная защита информации [Электронный ресурс]:Учебноепособие. - Москва: Издательство "ФОРУМ", 2026. - 352 с. – Режим доступа:https://znanium.com/catalog/product/2207457

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

PostgreSQL Server. Лицензия PostgreSQL. Срок действия лицензии - без ограничения срока.

Язык программирования Python.Python Software Foundation License (PSFL). Срок действия лицензии - без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к дифференцированному зачету

1. Что такое информационная безопасность и какие основные задачи она решает?
2. Какие этапы можно выделить в истории развития информационной безопасности?
3. Какие современные угрозы и риски наиболее характерны для информационных систем?
4. Какие нормативно-правовые документы регулируют вопросы информационной безопасности?
5. Для чего организации нужны политики и процедуры информационной безопасности?
6. Что такое риск в информационной безопасности и как проводится его оценка?
7. В чем различие между симметричными и асимметричными алгоритмами шифрования?
8. Для чего используются хэширование и цифровая подпись?
9. В каких случаях криптографические методы применяются в прикладных системах?
10. Что такое стеганография и чем она отличается от шифрования?
11. Какие основные угрозы существуют для сетевой инфраструктуры?
12. Какую роль играют VPN и межсетевые экраны в защите сети?
13. Какие уязвимости веб-приложений входят в число наиболее распространенных?
14. Что понимается под безопасным программированием и почему оно важно?
15. В чем различие между защитой данных в покое и защитой данных в транзите?
16. Для чего нужны резервное копирование и восстановление данных?
17. Какие особенности информационной безопасности характерны для облачных технологий?
18. Что включает процесс реагирования на инциденты информационной безопасности?
19. Почему социальная инженерия считается одной из самых опасных угроз?
20. Какие современные технологии и тенденции влияют на будущее информационной безопасности?

Приложение 2
к рабочей программе

7.3.2. Практические задания для самостоятельной подготовки к зачету
Тестовые задания

№ задания	Содержание задания	Правильный ответ
ОК 01: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам		
Закрытые вопросы		
1	Что такое информационная безопасность? А. Защита информации от угроз; Б. Только хранение файлов; В. Только установка антивируса; Г. Только работа в интернете	А
2	Что относится к угрозам информационной безопасности? А. Фишинг; Б. Резервное копирование; В. Архивирование; Г. Каталогизация	А
3	Целостность информации - это: А. Возможность быстро найти файл; Б. Защита данных от несанкционированного изменения; В. Передача данных по сети; Г. Хранение данных в облаке	Б
4	Целостность информации - это: А. Возможность быстро найти файл; Б. Защита данных от несанкционированного изменения; В. Передача данных по сети; Г. Хранение данных в облаке	Б
5	Что нужно сделать при обнаружении подозрительного письма? А. Открыть все вложения; Б. Проверить отправителя и не переходить по сомнительным ссылкам; В. Переслать письмо всем коллегам; Г. Сразу удалить почтовую программу	Б
Открытые вопросы		
1	Что такое информационная безопасность?	Защита информации от угроз и несанкционированного доступа
2	Что такое конфиденциальность?	Защита информации от посторонних лиц
3	Что такое целостность данных?	Сохранение данных без искажений и несанкционированных изменений
4	Что такое угроза информационной безопасности?	Возможность причинения

		вреда информации или системе
5	Как нужно действовать при получении подозрительного письма?	Проверить отправителя и не открывать сомнительные ссылки и вложения
ОК 02: Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности		
Закрытые вопросы		
1	Что такое фишинг? А. Метод резервного копирования; Б. Способ кражи данных через поддельные сообщения и сайты; В. Формат файла; Г. Вид шифрования	Б
2	Какой пароль считается более надёжным? А. 123456; Б. qwerty; В. P@ss2026!Sec; Г. ivan	В
3	Для чего нужна двухфакторная аутентификация? А. Для ускорения работы интернета; Б. Для дополнительной защиты учётной записи; В. Для сжатия файлов; Г. Для оформления документов	Б
4	Что из перечисленного лучше не делать в общественном Wi-Fi? А. Читать новости; Б. Входить в интернет-банк без защиты; В. Проверять погоду; Г. Искать расписание	Б
5	Что помогает защитить устройство от вредоносных программ? А. Отключение обновлений; Б. Антивирус и регулярные обновления; В. Удаление папок; Г. Выключение экрана	Б
Открытые вопросы		
1	Что такое фишинг?	Обман пользователя с целью получения его данных
2	Каким должен быть надёжный пароль?	Длинным, сложным и уникальным
3	Для чего нужна двухфакторная аутентификация?	Для дополнительной защиты учётной записи
4	Почему опасно пользоваться общественным Wi-Fi без защиты?	Данные могут быть перехвачены злоумышленниками
5	Что помогает защитить компьютер от вредоносных программ?	Антивирус и регулярные обновления системы
ОК 09: Пользоваться профессиональной документацией на государственном и иностранном языках		
Закрытые вопросы		
1	Что означает сокращение VPN?	А

	А. Защищённое сетевое соединение; Б. Формат документа; В. Вид вируса; Г. Способ архивации	
2	Что такое межсетевой экран? А. Программа для рисования; Б. Средство фильтрации сетевого трафика; В. Облачное хранилище; Г. Вид базы данных	Б
3	Что означает термин «аутентификация»? А. Удаление данных; Б. Проверка подлинности пользователя; В. Шифрование архива; Г. Резервное копирование	Б
4	Что такое вредоносное ПО? А. Программа, наносящая вред системе; Б. Только антивирус; В. Обычное офисное приложение; Г. Драйвер устройства	А
5	Что означает слово «backup» в ИБ? А. Сетевой протокол; Б. Резервная копия; В. Пароль; Г. Журнал событий	Б
Открытые вопросы		
1	Что такое VPN?	Защищённое соединение через сеть
2	Для чего нужен межсетевой экран?	Для фильтрации трафика и защиты сети
3	Что такое аутентификация?	Проверка личности пользователя
4	Что такое вредоносное ПО?	Программа, наносящая вред системе или данным
5	Что такое backup?	Резервная копия данных
ПК 1.1: Проектировать базы данных		
Закрытые вопросы		
1	Что помогает защитить данные при хранении? А. Шифрование; Б. Удаление ярлыков; В. Переименование файлов; Г. Смена обоев	А
2	Для чего нужно резервное копирование? А. Для удаления старых файлов; Б. Для восстановления данных после сбоя; В. Для ускорения интернета; Г. Для смены формата файла	Б
3	Кто должен иметь доступ к конфиденциальным данным? А. Все сотрудники; Б. Только уполномоченные пользователи; В. Любой посетитель; Г. Все пользователи интернета	Б
4	Что из перечисленного лучше хранить в зашифрованном	Б

	виде? А. Публичную рекламу; Б. Персональные данные; В. Открытое расписание; Г. Инструкцию по технике безопасности общего доступа	
5	Что помогает обнаружить несанкционированный доступ к данным? А. Журналы событий; Б. Цвет папки; В. Размер монитора; Г. Имя компьютера	А
	Открытые вопросы	
1	Что защищает данные при хранении?	Шифрование и ограничение доступа
2	Зачем нужно резервное копирование?	Для восстановления данных после потери или сбоя
3	Кто должен иметь доступ к конфиденциальной информации?	Только уполномоченные пользователи
4	Какие данные особенно важно защищать?	Персональные, финансовые и служебные данные
5	Что помогает выявлять попытки доступа к данным?	Журналы событий и аудит
ПК 1.4: Администрировать базы данных		
	Закрытые вопросы	
1	Какая атака часто используется против баз данных через веб-приложение? А. SQL-инъекция; Б. Форматирование текста; В. Архивация; Г. Индексация	А
2	Что снижает риск несанкционированного доступа к базе данных? А. Открытый доступ из интернета; Б. Разграничение прав пользователей; В. Одинаковый пароль для всех; Г. Отключение аутентификации	Б
3	Что помогает защитить соединение с базой данных? А. Шифрование канала связи; Б. Переименование таблиц; В. Удаление резервных копий; Г. Выключение сервера	А
4	Что помогает выявить попытки атак на базу данных? А. Мониторинг и журналирование; Б. Удаление логов; В. Смена названия БД; Г. Отключение сети	А
5	Что уменьшает риск SQL-инъекции? А. Проверка вводимых данных; Б. Отключение антивируса; В. Сжатие базы; Г. Удаление индексов	А
	Открытые вопросы	
1	Какая атака часто направлена на базу данных через сайт?	SQL-инъекция

2	Что помогает ограничить доступ к базе данных?	Разграничение прав пользователей
3	Как защитить соединение с базой данных?	Использовать шифрование канала связи
4	Что помогает выявлять атаки на БД?	Мониторинг и журналирование
5	Что уменьшает риск SQL-инъекций?	Проверка входных данных и безопасные запросы
ПК 1.5: Защищать информацию в базе данных с использованием технологии защиты информации		
Закрытые вопросы		
1	Что используется для защиты данных при передаче через сайт? А. HTTPS/TLS; Б. TXT; В. BMP; Г. CSV	А
2	Что подтверждает подлинность электронного документа? А. Цифровая подпись; Б. Архивирование; В. Сжатие файла; Г. Переименование	А
3	Что лучше использовать для безопасного входа в систему? А. Простой пароль; Б. Двухфакторную аутентификацию; В. Общую учётную запись; Г. Вход без пароля	Б
4	Какой протокол применяется для безопасного удалённого доступа к серверу? А. SSH; Б. HTTP; В. FTP; Г. Telnet	А
5	Что из перечисленного связано с защитой персональных данных? А. GDPR; Б. JPEG; В. HTML; Г. ZIP	А
Открытые вопросы		
1	Что защищает веб-трафик пользователя?	HTTPS или TLS
2	Что обеспечивает цифровая подпись?	Подлинность и целостность документа
3	Что повышает безопасность входа в систему?	Двухфакторная аутентификация
4	Какой протокол используют для безопасного доступа к серверу?	SSH
5	Что регулирует GDPR?	Защиту и обработку персональных данных
ПК 3.1: Собирать исходные данные для разработки проектной документации на		

информационную систему		
Закрытые вопросы		
1	Какой стандарт часто используют при построении системы управления ИБ? А. ISO 27001; Б. JPEG; В. PNG; Г. MP4	А
2	Что относится к профессиональным источникам информации по ИБ? А. Нормативные документы и техническая документация; Б. Случайные комментарии; В. Развлекательные ролики; Г. Рекламные баннеры	А
3	Что помогает специалисту выбрать актуальные меры защиты? А. Анализ нормативных документов и современного опыта; Б. Только слухи; В. Только старые инструкции; Г. Случайный выбор	А
4	Что относится к отраслевой документации? А. Регламенты и стандарты; Б. Художественный рассказ; В. Рекламный пост; Г. Личная переписка	А
5	Почему важно использовать официальные документы в ИБ? А. Они содержат проверенные требования и правила; Б. Они всегда короче; В. Они не требуют проверки; Г. Они заменяют обучение	А
Открытые вопросы		
1	Почему важно изучать современный опыт в ИБ?	Он помогает применять актуальные методы защиты
2	Какой стандарт часто применяют в управлении ИБ?	ISO 27001
3	Какие источники информации нужны специалисту по ИБ?	Нормативные документы, стандарты и техническая документация
4	Что относится к отраслевой документации?	Регламенты, инструкции и стандарты
5	Почему лучше использовать официальные источники?	Они надёжны и содержат проверенные требования
ПК 3.3: Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием		
Закрытые вопросы		
1	Что нужно учитывать при анализе безопасности информационной системы? А. Угрозы и риски; Б. Только цвет интерфейса;	А

	В. Только размер жёсткого диска; Г. Только название программы	
2	Что помогает определить требования к защите системы? А. Анализ возможных атак; Б. Случайный выбор средств; В. Только мнение одного пользователя; Г. Игнорирование документации	А
3	Что важно учитывать при защите персональных данных? А. Законодательные требования; Б. Только объём памяти; В. Только модель принтера; Г. Только количество сотрудников	А
4	Что является результатом анализа требований безопасности? А. Набор мер защиты; Б. Только имя администратора; В. Только дата проверки; Г. Только список файлов	А
5	Что важно учитывать в системе с разными категориями пользователей? А. Роли и уровни доступа; Б. Только название учётной записи; В. Только размер экрана; Г. Только номер кабинета	А
Открытые вопросы		
1	Что учитывают при анализе безопасности системы?	Угрозы, риски и состав защищаемой информации
2	Что помогает определить меры защиты?	Анализ угроз и уязвимостей
3	Что важно учитывать при защите персональных данных?	Требования законодательства и характер данных
4	Что является результатом анализа требований безопасности?	Перечень мер и требований к защите
5	Почему важно учитывать роли пользователей?	Чтобы правильно разграничить доступ
6	Что такое уязвимость информационной системы?	Слабое место, через которое можно нарушить безопасность
7	Что такое риск в информационной безопасности?	Вероятность и последствия реализации угрозы
8	Что такое мера защиты?	Способ предотвращения или снижения угрозы
9	Что помогает снизить риск утечки данных?	Ограничение доступа и контроль действий пользователей
10	Почему важно анализировать угрозы заранее?	Чтобы заранее выбрать подходящие меры защиты
ПК 3.6: Осуществлять модульное и интеграционное тестирование информационной системы		
Закрытые вопросы		
1	Что помогает обнаружить попытку взлома сети? А. Система обнаружения вторжений; Б. Текстовый редактор; В. Табличный процессор;	А

	Г. Графический редактор	
2	Что лучше использовать для защиты сети организации? А. Межсетевой экран; Б. Плеер; В. Сканер документов; Г. Архиватор	А
3	Что помогает защитить устройство от известной уязвимости? А. Установка обновлений; Б. Отключение системы; В. Удаление ярлыков; Г. Переименование папок	А
4	Что помогает вовремя заметить инцидент безопасности? А. Мониторинг событий; Б. Выключение логов; В. Очистка корзины; Г. Смена заставки	А
5	Что из перечисленного относится к мерам защиты инфраструктуры? А. Антивирус и межсетевой экран; Б. Только архивирование; В. Только печать документов; Г. Только копирование файлов	А
Открытые вопросы		
1	Что помогает обнаружить попытки вторжения в сеть?	Система обнаружения вторжений
2	Что защищает сеть организации от нежелательного трафика?	Межсетевой экран
3	Что помогает закрывать известные уязвимости?	Регулярные обновления
4	Что помогает вовремя заметить инцидент ИБ?	Мониторинг и журналы событий
5	Какие средства часто используют для защиты инфраструктуры?	Антивирусы, межсетевые экраны и системы мониторинга

Практические задания к дифференцированному зачету

Практическое задание
Провести анализ парольной политики для заданной организации и предложить рекомендации по её улучшению.

Практическое задание
Распознать признаки фишингового письма в предложенном примере и объяснить, какие элементы указывают на попытку мошенничества.

Практическое задание
Для предложённого набора данных определить, какие сведения являются конфиденциальными, какие - общедоступными, а какие требуют ограничения доступа.

Практическое задание
Сравнить два способа защиты данных при хранении и передаче информации и сделать вывод, в каких случаях каждый из них более уместен.

Практическое задание
Для заданной сетевой схемы определить уязвимые места и предложить меры защиты с использованием межсетевого экрана, VPN или сегментации сети.

Практическое задание
Проанализировать ситуацию утечки данных и составить краткий план реагирования на инцидент информационной безопасности.

Практическое задание
Для заданной ситуации предложить схему разграничения прав доступа пользователей к данным и кратко обосновать выбранное решение.

Практическое задание
Проанализировать журнал событий или описание событий безопасности и определить, какие из них могут свидетельствовать о подозрительной активности.

Практическое задание
Определить, какие методы аутентификации и авторизации целесообразно использовать в заданной информационной системе, и объяснить свой выбор.

Практическое задание
Сопоставить предложенные меры защиты с видами угроз: вредоносное ПО, несанкционированный доступ, социальная инженерия, перехват данных, утрата информации.